Data Breach Policy

Destination NSW has adopted this Data Breach Policy developed by The Department of Creative Industries, Tourism, Hospitality and Sport (DCITHS). This Policy outlines how it will deal with data breaches involving personal information.

Table of Contents

1. Introduction

This Data Breach Policy (**Policy**) sets out an overview of Destination NSW (the **Agency, DNSW, us, we** or **our**) procedures in relation to detecting, responding to, managing notifying and reporting eligible data breaches in accordance with the Mandatory Notification of Data Breach Schedule (**the MNDB Scheme**) under Part 6A of the Privacy and Personal Information Protection Act 1998 (NSW) (**PPIP Act**).

This policy complies with section 59ZD of the PPIP Act. This Policy provides a framework for DNSW's compliance with MNDB Scheme.

Staff should consult internal procedures for detailed guidance on how to respond to a data breach in accordance with this Policy.

The purpose of this Policy is to set out how DNSW will respond to data breaches involving personal information. While not all data breaches will be eligible data breaches, DNSW takes all data breaches seriously and will assess each data breach in accordance with this Policy.

2. Definitions

Term	Definition
Data Breach Response Team	is the team consisting of senior DNSW personnel responsible for coordinating and managing DNSW's response to a data breach.
data breach	occurs when information held by an agency (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure, or any accidental or unlawful destruction or alteration of personal information held by (or on behalf of) DNSW.
Data Breach Response Plan	means a detailed internal plan outlining the steps required for DNSW staff to contain, assess, investigate and respond to a data breach.
eligible data breach	means a data breach which has satisfied the following two tests under the MNDB Scheme: 1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information; and 2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.
health information	means any personal information that is information or an opinion about a person's physical or mental health or disability or the provision of health services to them, including an individual's express wishes about the future provision of health services to them. It also includes genetic information that is or could be predictive of the health of a person or their genetic relative as well as any personal information that was collected to provide, or in providing, a health service, or in connect with donation of body parts, organs or body substances (section 6 of the Health Records and Information Privacy Act 2002 (NSW) (HRIP Act).

Term	Definition
likely to result in serious harm	'likely' means the risk of serious harm to an individual is more probable than not. To help assess this it is the likelihood that an individual might suffer serious harm if their personal information was lost, or subject to unauthorised access or unauthorised disclosure.
MNDB Scheme	has the meaning of the Mandatory Notification of Data Breach Scheme established in Part 6A of the PPIP Act, commenced 28 November 2023.
personal information	means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion (see section 4 of the PPIP Act). The definition of personal information for the purposes of the MNDB Scheme includes 'health information', as defined in section 6 of the HRIP Act. This means that for the purposes of the MNDB Scheme (Part 6A of the PPIP Act only), 'personal information' includes information about an individual's physical or mental health, disability, and information connected to the provision of a health service. For the purposes of this Policy, unless other noted, personal information includes 'health information'.
serious harm	occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience. Harm to individual includes serious physical, psychological, emotional, financial or reputational harm. Examples of harms include identity theft, financial loss or blackmail, threats to personal safety, loss of business or employment opportunities, humiliation, stigma, embarrassment, damage to reputation or relationships, discrimination, bullying, marginalisation, or other forms of disadvantage or exclusion.
staff	All DNSW permanent full time, part time, volunteer, trainee and temporary employees and staff authorised to access DNSWi nformation systems and assets. Any consultants and persons or organisations authorised to administer, develop, manage and support DNSW information systems and assets. Any third party supplier, vendors, contractors and hosted managed service providers.

3. Scope

This Policy applies to and must be adhered to and implemented by:

- all DNSW permanent full time, part time, volunteer, trainee and temporary employees and staff authorised to access DNSW information systems and assets;
- any consultants and persons or organisations authorised to administer, develop, manage and support DNSW information systems and assets; and
- third party supplier, vendors, contractors and hosted managed service providers.

All Staff have a responsibility to notify the Director Legal, Procurement and Governance of any data breach immediately on becoming aware that a data breach has occurred and provide information about the data breach in accordance with procedures.

4. What is an eligible data breach?

A data breach occurs when there has been unauthorised access to, unauthorised disclosure of or loss of personal information (including health information) held by (or on behalf of) DNSWDNSW or any accidental or unlawful destruction or alteration of personal information held by (or on behalf of) DNSWDNSW.

A data breach may occur as the result of a malicious action, systems failure or human error. A data breach may occur also because of misconception as to whether a particular act or practice is permitted under PPIP Act.

Examples of data breaches include:

- **Malicious or criminal attack**
  - Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
  - Social engineering or impersonation leading into inappropriate disclosure of personal information. Insider threats from agency employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
  - Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.
- **System fault**
  - Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.
  - Where systems are not maintained through the application of known and supported patches.

- **Human error**
  - When a letter or email is sent to the wrong recipient.
  - When system access is incorrectly granted to someone without appropriate authorisation. When a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information is lost or misplaced.
  - When staff fail to implement appropriate password security, for example not securing passwords or sharing password and log in information.

If there are reasonable grounds to believe that the data breach has resulted in, or is likely to result in, serious harm to one or more of the individuals to whom the information relates, the data breach is an 'eligible data breach'.

Serious harm occurs where harm arising for the eligible data breach has or could result in a real and substantial detrimental the effect on an individual and includes serious physical, psychological, emotional, financial, or reputational harm. Examples of harms include identity theft, financial loss or blackmail, threats to personal safety, loss of business or employment opportunities, humiliation, stigma, embarrassment, damage to reputation or relationships, discrimination, bullying, marginalisation, or other forms of disadvantage or exclusion.

Assessment of the likelihood of serious harm from a data breach is an objective test. That is **'likely to result'** (as defined above) means the risk of serious harm to an individual is more probable than not.

5. Process for managing a data breach

DNSW takes reasonable security safeguards against the loss, unauthorised access, use, modification and disclosure of personal information. DNSW has established a range of policies and processes for preventing and managing data breaches.

DNSW has a Data Breach Response Plan for detailed guidance on how to respond to a data breach in accordance with this Policy.

DNSW has in place information security policies which provide guidance to staff around the handling and storage of personal information. For example, DNSW's Code of Ethics and Conduct for staff and contractors has specific provisions on privacy obligations, including in relation to the authorised access, disclosure and storage of personal information. The Code also has provisions on the handling of information, including in relation to the confidentiality, misuse and security of information, and on records management. We comply with the Information Security Policy from the Department of Creative Industries, Tourism, Hospitality and Sport (https://intranet.enterprise.nsw.gov.au/business-support/deit-policies/information-security-policy/) which has provisions on information access and security and that staff must use information on a 'need to see basis'.

DNSW's security measures further include the use of restricted drives and authorised access.

Personal information is kept for no longer than is necessary and is disposed of in a secure manner once no longer required, in accordance with government requirements.

6. Data breach response and reporting

DNSW will consider a number of factors in assessing a data breach including the NSW Privacy Commissioner's statutory guidelines and will engage the following steps in response to all data breaches:

Step 1: Contain the data breach and conduct a preliminary assessment

- Immediately take all realistic steps to contain the breach and limit any further access or distribution of the affected personal information.
- Conduct preliminary fact-finding about the breach.
- Make a preliminary assessment of the risk posed by the data breach.
- For high risk rated data breaches, the Director Legal, Procurement and Governance will activate and escalate to the Data Breach Response Team to oversee the remainder of the response.

The **Data Breach Response Team** will consist of:

- The Chief Executive Officer (CEO) with responsibility for final approval on decisions and proposals by the Data Breach Response Team.
- Director Legal, Procurement and Governance who will lead the assessment, mitigation and notification of the data breach.
- Senior Legal Counsel and Legal and Governance Advisor who will identify and advise on any legal obligations and support the drafting of notifications and communications issued under this Policy.
- Director Corporate Systems and Delivery and General Manager, Corporate Services who will liaise with any related ICT partners as required to obtain and provide information into the cause and impacts of the data breach.
- Any internal or external expertise and incident response advisors the Data Breach Response Team determines are required to complete the assessment and mitigation of the data breach.

Step 2: Evaluate and mitigate the risks associated with the data breach

- As soon as practicable, take remedial action to prevent or lessen the likelihood that the breach will result in harm to any individual.
- Complete an assessment of the harm that may eventuate from the breach
- Consider requirements under any third party agreements and third party organisations or agencies whose data may be affected

- For high risk data breaches, the Data Breach Response Team should consider whether to involve any other internal or external parties such as:
    - ID Support
    - law enforcement agencies, NSW Police Force and/or Australian Federal Police
    - IDCare
    - Financial services providers
    - Professional associations, regulatory bodies
    - The Office of Australian Information Commission where data breach may involve tax file numbers or agencies under Federal jurisdiction
    - Cyber Security NSW, and/or the Australian Cyber Security Centre.

Step 3: Notify and communicate

- If the breach is assessed as eligible data breach, on the advice of the Breach Response Team, the appropriate communications messaging templates and procedures in the Data Breach Response Plan will be used to notify the Privacy Commissioner and affected individuals where required.
- Notification is required by law under the PPIP Act and may also be required under Federal Privacy Act 1988 (Cth).
- In accordance with section 59O of PPIP Act, the notification will include the following specific information, if reasonably practicable:
    - The date the data breach occurred
    - A description of the data breach
    - How the data breach occurred
    - The type of data breach that occurred
    - The personal information included in the data breach
    - The amount of time the personal information was disclosed for
    - Actions that have been taken or are planned to secure the information, or to control and mitigate the harm
    - Recommendations about the steps an individual should take in response to the data breach
    - Information about complaints and review of agency conduct
    - The name of the agencies that were subject to the data breach
    - Contact details for the agency subject to the data breach or the nominated contact person in relation to the data breach

Step 4: Prevent future data breaches

- For any high risk or medium risk breaches the Director Legal, Procurement and Governance will submit a report to the Data Breach Response Team outlining the organisational response and mitigation plan.

- A post incident review of the process used for the data breach, after it has been handled, will be conducted, reported to the Data Breach Response Team and the Chief Executive Officer with details of any recommendations.

Step 5: Record keeping requirements

- DNSW will maintain an internal register of all eligible date breaches impacting DNSW.
- DNSW will maintain a public notification register on the DNSW website. This will be a public notification register of eligible data breaches where DNSW is unable to notify, or it is not reasonably practicable to notify affected individuals.

For further detailed requirements of our internal and external reporting, DNSW staff must consult our Data Breach Response Plan.

7. DNSW staff awareness

To ensure that DNSW staff are and remain aware of their obligations under the MDNB Scheme, DNSW will:

- prepare and notify staff of this Policy and any additional training and publish it and any additional relevant awareness material in a prominent place on the DNSW intranet;
- provide training on this Policy to raise awareness and appreciation of these privacy obligations generally;
- provide refresher and on-the-job training as required;
- highlight and promote the Policy; and provide privacy briefing and awareness
- sessions in appropriate Senior Executive forums.

8. Further information and contacts

For further information about this Policy, an eligible data breach on the public notification register or if you have any concerns, please contact the Director Legal, Procurement and Governance:

Director Legal, Procurement and
Governance
Destination NSW
Level 2, 88 Cumberland St, The Rocks NSW 2000
Email: Legal.Procurement@dnsw.com.au

For more information on privacy rights and obligations in New South Wales, please contact the NSW Privacy Commissioner at:

NSW Information and Privacy Commission Level
17, 201 Elizabeth Street
Sydney NSW 2000

Phone: 1800 472 679

Web: www.ipc.nsw.gov.au

Email: ipcinfo@ipc.nsw.gov.au

Variation

Destination NSW may amend this policy from time to time as appropriate.

Latest Version	**Next Review Date**
21 December 2023	21 December 2024